CLAIMS:

What is claimed is:

1. A method for the containment of a virus in a computer network, comprising evaluating an outgoing message from a computer device and blocking the transmission of the message if it does not conform to an established list of permitted actions.

2. A method for the containment of a virus in a computer network, comprising:

(a) establishing a list of permitted operations in a computer network;

(b) intercepting a message emanating from a device in the computer network;

(c) comparing the intercepted message to the list of permitted operations;

(d) transmitting the message if the message conforms to one of the permitted operations on the list; and

(e) blocking the message if the message does not conform to one of the permitted operations on the list.

3. The method for the containment of a virus in a computer network as described in claim 2, wherein the list of permitted operations comprises permitting transmission only to another network or computer device having one of certain addresses or protocols.

4. The method for the containment of a virus in a computer network as described in claim 2, wherein the list of permitted operations comprises transmission to another network or computer device only in response to an external initiation.

5. The method for the containment of a virus in a computer network as described in claim 2, wherein one of the permitted operations comprises establishing communications between two servers or the like devices.

6. The method for the containment of a virus in a computer network as described in claim 2, further comprising transmitting the message only if the message conforms to a first and a second of the permitted operations on the list.

7. A firedoor system for the containment of a virus in a computer network, comprising a firedoor for receiving a message from a computer device, comparing the received message to an established list of permitted operations and transmitting the received message only if it conforms to the list of permitted operations.

8. A firedoor system for the containment of a virus in a computer network, comprising:

(a) a firewall connected to the computer network so as to receive messages from an outside source and adapted for screening unwanted messages;

(b) a computer device connected to receive messages passed by the firewall; and

(c) a firedoor connected to the computer device so as to receive messages from the computer device and to evaluate the received messages and transmit only permitted messages to other computer devices in the computer network.

9. The firedoor system for the containment of a virus in a computer network as described in claim 8, wherein the firedoor is connected to an output port of the computer device.

10. The firedoor system for the containment of a virus in a computer network as described in claim 8, wherein the firedoor is connected to a computer network bus.

11. The firedoor system for the containment of a virus in a computer network as described in claim 8, wherein the firedoor is connected to a computer network channel.

12. The firedoor system for the containment of a virus in a computer network as described in claim 8, wherein the firedoor is provided in series with a second firedoor so that different verification criteria from each firedoor are applied serially.

4005985.1